Administration Guide

FortiVoice Gateway 7.0.6

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change log

Date	Change description
2025-02-11	Initial release of the FortiVoice Gateway 7.0.6 Administration Guide.

Introduction

The FortiVoice Gateway is a simple solution for adding analog phone lines (GO04, GO08, GS04, GS16, and GS24) or PRI lines (GT01 and GT02) to your SIP server enabled PBX. With the easy to use and intuitive web interface, you can quickly create rules that allow calls from analog/PRI lines, connected to the FortiVoice Gateway FXO/PRI ports, to communicate directly to your SIP server enabled PBX. The FortiVoice Gateway also offers various usage tracking options, such as call statistics and call detail records, so you can monitor the calls coming through the system.

This document describes how to configure and use the FortiVoice Gateway through the GUI.

> Prior to configuring the FortiVoice Gateway, make sure to deploy the FortiVoice Gateway first. See details in one of the following documents:
> - FortiVoice FXO Gateway Deployment Guide
> - FortiVoice FXS Gateway Deployment Guide
> - FortiVoice PRI Gateway Deployment Guide

This section includes the following topics:

- Registering your Fortinet product on page 6
- Training on page 7
- Documentation on page 7
- Scope on page 7
- Conventions on page 8

Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product.

Many Fortinet customer services, such as firmware updates and technical support, require product registration.

> Registering products is only available to master users and sub-users with full access permissions.

To register your Fortinet product

1. Go to Fortinet Support website.
2. Log in to your existing account or register for an account.
3. Click **Register Now**.
4. Follow the prompts to complete the product registration.

Customer service and support

Fortinet Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Support website.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing a clear problem description, the latest gateway configuration file, the latest gateway debug log file, and a network diagram.

Training

Fortinet Training Service provides classes that orientate you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Service or send an email to training@fortinet.com.

Documentation

The Fortinet Document Library provides the most up-to-date versions of Fortinet product publications.

Fortinet Knowledge Base

In addition to the Fortinet Document Library, you can visit the Fortinet Knowledge Base.

The Fortinet Knowledge Base includes troubleshooting and how-to articles, examples, FAQs, and technical tips.

Feedback on Fortinet technical documentation

Please send information about any errors or omissions in this document to techdoc@fortinet.com.

Scope

The majority of procedures in this document use the GUI to configure the FortiVoice Gateway unit and perform other tasks. Some tasks use the CLI.

Conventions

Fortinet technical documentation uses the following conventions:

- IP addresses on page 8
- Cautions and notes on page 8
- Typographical conventions on page 8

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Cautions and notes

Fortinet technical documentation uses the following guidance and styles for cautions and notes.

> Warns you about commands or procedures that could have unexpected or undesirable results, including loss of data or damage to equipment.

> Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Style	Description	Example
Italic font	Used for GUI navigation.	From *Minimum log level*, select *Notification*. Go to *Phone System > Setting > Location*.
`Courier` font and indentation	Used for CLI input.	```config system dns set primary <address_ipv4> end```
`Courier` font	Used for CLI output.	`FGT-602803030703 # get system Setting`

Style	Description	Example
		comments : (null) opmode : nat
`Courier` font	Used for file content.	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>`
`Courier` font	Used for text that you type.	Type a name for the remote VPN peer or client, such as `Central_Office_1.`
Blue font	Used for hyperlinks to websites and publications.	Visit the Fortinet Support website. For details, see the FortiVoice User Portal Guide.
<text_in_angle_ brackets>	Describes a variable. Replace the <text_in_angle_brackets> with the required information for your setup. Do not type the angle brackets.	FortiVoice user portal link: https://<IP_address_or_ FQDN>/voice

Logging in to the FortiVoice Gateway GUI

Log in to the GUI of the FortiVoice Gateway by using the IP address, administrative access protocol, administrator account, and password that you configured during the FortiVoice Gateway deployment.

Prerequisites

- Deploy the FortiVoice Gateway. For details, see one of the following documents:
  - FortiVoice FXO Gateway Deployment Guide
  - FortiVoice FXS Gateway Deployment Guide
  - FortiVoice PRI Gateway Deployment Guide
- Know the IP address or FQDN (and access port, if required) of the FortiVoice Gateway.
- Know the account name and associated password to connect to the FortiVoice Gateway.
- Use one of the recommended web browsers:
  - Google Chrome version 132
  - Microsoft Edge version 132
  - Mozilla Firefox Standard Release version 134
  - Apple Safari version 18.2

To log in to the FortiVoice Gateway GUI

1. Start a web browser and go to :
   ```
   https://<IP_address>/admin
   ```
   Where <IP_address> is the IP address of the FortiVoice Gateway that you want to connect to. If the FortiVoice Gateway configuration is using a non-default HTTPS port, add `:<port_number>` after the IP address. For example:
   ```
   https://<IP_address>:446/admin
   ```
2. Enter the name and password associated with the account.
3. Click **Log In**.
   The GUI page of the FortiVoice Gateway opens.

Using the dashboard

The *Dashboard* displays system statuses, most of which pertain to the entire system, such as CPU usage and mail statistics.

This section includes the following topics:

- Viewing the dashboard on page 11
- Viewing Call Statistics on page 12
- Accessing the CLI console on page 12

Viewing the dashboard

The *Dashboard > Status* displays first after you log in to the web UI. It contains a dashboard with widgets that indicate performance level or other statistics.

By default, widgets display the serial number and current system status of the FortiVoice Gateway unit, including uptime, system resource usage, license information, service status, firmware version, system time, and statistics history.

To view the dashboard, go to *Dashboard > Status*.

This topic includes Hiding, showing and moving widget on page 11.

Hiding, showing and moving widget

The dashboard is customizable. You can select which widgets to display, where they are located on the tab, and whether they are minimized or maximized.

To move a widget, position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To show or hide a widget select *Manage Widget* and then select the widgets you want to display on the Dashboard. If the widget is greyed out, the widget will not display. Select *Apply* when you have made your selections.

Options vary slightly from widget to widget, but always include options to close, refresh, or minimize/maximize the widget.

System Information widget

The *System Information* widget displays the serial number and basic system statuses such as the firmware version, system time, and uptime.

In addition to displaying basic system information, the *System Information* widget lets you change the firmware. To change the firmware, click *Update* for *Firmware version*. For more information, see Installing the firmware on page 66.

System Resource widget

The *System Resource* widget displays the following information:

- CPU usage
- Memory usage
- Log disk usage
- Storage usage
- System load

The system resources history can also be viewed in this widget by clicking *History*. The system resources history contains four graphs. Each graph displays readings of one of the system resource usages: CPU, memory, session, and network. Each graph is divided by a grid.

Statistics History widget

The *Statistics History* widget contains charts that summarize the number of calls in each time period that the FortiVoice Gateway unit has recorded.

See also .

Service Status widget

The *Service Status* widget displays details such as the number of active calls, trunk status, endpoint count, and device connection status.

The *Device* list displays the connection status of the FortiVoice Gateway physical ports:

- *Connected* 🔗 : The port is connected to a device.

- *Disconnected* 🔗 : The port is not connected to any device and is in an alarm state.

- *Occupied* 📞 : The port is being used.

- *Information* ⓘ : The port has an other status.

Viewing Call Statistics

The *Dashboard > Call Statistics* tab contains summaries of the number of calls by time (minute, hour, day, month, and year) and direction (incoming, outgoing, and internal) that the FortiVoice Gateway unit recorded.

Accessing the CLI console

To access the CLI without exiting from the web UI, go to *Dashboard > Console*.

To move the CLI console into a pop-up window that you can resize and reposition, go to the bottom of the page and click the *Open in New Window* button.

Monitoring the FortiVoice Gateway

The *Monitor* menu displays system usage, log messages, and other status-indicating items.

This section includes the following topics:

Viewing phone system status

The *Monitor > Phone System* displays all the ongoing phone calls and trunks.

This topic includes:

Viewing active calls

Monitor > Phone System > Active Call displays all the ongoing phone calls in realtime, including the callers and receivers, the trunks through which phone calls are connected, the call status, and the call duration.

You can stop a phone call by clicking *Hang up* 📞 .

The call statuses include:

- *Ringing*: The receiver's phone is ringing.
- *Connected*: Callers are connected. The voice channel is established.
- *Voicemail*: The call goes to the voicemail.

Viewing trunk status

Monitor > Phone System > Trunk displays all the trunks in realtime, including their names, IP addresses, types, status, and registration/connection status with the VoIP or public switched telephone network (PSTN) service provider.

Status can show the following conditions:

- *Not registered*: The trunk is not registered with the VoIP or PSTN service provider and is not in service.
- *In service*: The trunk is registered with the VoIP or PSTN service provider and is in service.
- *Unavailable*: The trunk is not reachable.
- *Alarm detected*: There is a problem with the trunk.
- *Admin down*: The trunk is disabled.
- *Unmonitored*: The trunk is not monitored.

You can stop a phone call by clicking the *Hang Up* icon.

Registration/Connection indicates if a trunk has been registered with or connected to the VoIP or PSTN service provider. *Registration/Connection* can show the following icons:

- ✅ : The trunk is registered. (This icon is for the SIP trunk, office peer, and gateway only.)
- 🚫 : The trunk is OK. (This icon is for the PSTN only.)
- ✴ : The trunk or trunk channel has a red alarm. (This icon is for the PSTN only.)
- 📞 : The trunk or trunk channel is in service. (This icon is for the PSTN only.)
- ⚠ : The trunk or trunk channel has an alarm. (This icon is for the PSTN only.)

For configuration details, see Configuring the FortiVoice Gateway on page 42.

Viewing call detail records

The *Monitor > Call History* displays the call detail record (CDR) for phone calls made during a certain time period, including the time of the call, caller and receiver, call duration, call status, and call direction.

To display the detailed call information, including the call flow, double-click on the call record.

To filter the call history display, you can make selections in the *Direction* and *Disposition* drop-down lists and also enter criteria in the search field.

To download all call records

1. Click *Download > All*.
2. If the downloaded file shows # characters, expand the column to show all the text.

To download call records from a search

1. Enter a search string and press *Enter*.
2. If you want to download call records with their call flow, then set *With call flow* to *On*.
3. Click *Download > Search Result*.
4. To confirm, click *OK*.
5. If the downloaded file shows # characters, expand the column to show all the text.

Viewing log messages

The *Monitor > Log* displays locally stored log files. If you configured the FortiVoice Gateway to store log messages locally (that is, to the hard disk), you can view the log messages currently stored in each log file.

Logs stored remotely cannot be viewed from the GUI of the FortiVoice Gateway. If you want to view logs from the GUI, also enable local storage. For details, see Configuring logs on page 59.

Monitor > Log displays the logs of administrator activities and system events as well as voice and fax.

To view the list of log files and their contents

1. Go to *Monitor > Log > System/Voice/Fax.*
   The list of log files appears with the beginning and end of a log file's time range and the size of a log file in bytes. The queue log files display more information.
2. To search the log files, click the *Search* button and enter criteria that records must match in order to be visible. Unlike the search when viewing the contents of an individual log file, this search displays results regardless of which log file contains them. For more information, see Searching log messages on page 16.
3. To view messages contained in logs, double-click a log file.

Displaying and arranging log columns

When viewing logs, you can display, hide, sort and re-order columns.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see Searching log messages on page 16.

By default, each page's worth of log messages is listed with the log message with the lowest index number towards the top.

To sort the page entries in ascending or descending order

1. Click the column heading by which you want to sort.
   The log messages are sorted in ascending order.
2. To sort in descending order, click the column heading again.
   Depending on your currently selected theme:
   - The column heading may darken in color to indicate which column is being used to sort the page.
   - A small upwards-or downwards-pointing arrow may appear in the column heading next to its name to indicate the current sort order.

To show or hide columns

1. Go to *Monitor > Log > System/Voice/Fax*.
2. Click *Configure View* .
3. Click *Show/Hide Columns*.
4. Select the columns you want to show or hide.
5. Click *OK*.

To change the order of the columns

1. Go to *Monitor > Log > System/Voice/Fax*.
2. For each column whose order you want to change, click and drag its column heading to the left or right.
3. Click *Configure View* .
4. Click *Save View*.

Using the right-click pop-up menus

When you right-click on a log message, a context menu appears.

View Details	Select to display the log details.

Select All	Select to select all log messages in the current page. You can export all messages.
Clear Selection	Select to deselect one or multiple log messages.
Export	Select to open or save the log file.

Searching log messages

You can search logs to quickly find specific log messages in a log file, rather than browsing the entire contents of the log file.

To search log messages

1. Go to *Monitor > Log > System/Voice/Fax*.
2. Click *Search*.
3. Enter your search criteria by configuring one or more of the following:

GUI field	Description
Keyword	Enter any word or words to search for within the log messages. For example, you can enter `GUI session` to locate all log messages containing that exact phrase in any log field.
Message	Enter all or part of the *Message* log field.
Log ID	Enter all or part of the log ID in the log message.
Match condition	• *Contain*: Searches for the exact match. • *Wildcard*: Supports wildcards in the entered search criteria.
Start time End time	Select the date and time span of log messages to include in the search results.

4. Click *Search*.
   The FortiVoice Gateway unit searches for log messages that match your search criteria, and displays any matching log messages.

Configuring system settings

The *System* menu lets you configure of the FortiVoice Gateway operation system, including administrator accounts, network settings, system time, SIP settings, system maintenance, and more.

This section includes the following topics:

About FortiVoice Gateway logical interfaces

In addition to the physical interfaces, you can create the following types of logical interfaces on the FortiVoice Gateway:

VLAN subinterfaces

A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows the forwarding of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

VLANs use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

For information about adding VLAN subinterfaces, see Configuring the network interfaces on page 18.

Redundant interfaces

On the FortiVoice Gateway, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have

more robust configurations with fewer possible points of failure. This is important in a fully-meshed high availability (HA) configuration.

A physical interface is available to be in a redundant interface if the following conditions are met:

- The physical interface is not a VLAN interface.
- The physical interface is not already part of a redundant interface.
- The physical interface has no defined IP address and is not configured for DHCP.
- The physical interface does not have any VLAN subinterfaces.
- The physical interface is not monitored by HA.

When a physical interface is included in a redundant interface, it is not listed on the *System > Network > Network* page. You cannot configure the interface anymore.

For more information about adding redundant interfaces, see Configuring the network interfaces on page 18.

Loopback interfaces

A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.

The loopback IP address of the FortiVoice Gateway does not depend on one specific external port, and it is therefore possible to access it through several physical or VLAN interfaces. In the current release, you can only add one loopback interface on the FortiVoice Gateway.

For information about adding a loopback interface, see Configuring the network interfaces on page 18.

Configuring network settings

The *System > Network* provides options to configure network connectivity and administrative access to the GUI or CLI of the FortiVoice Gateway through each network interface.

This topic includes:

- Configuring the network interfaces on page 18
- Configuring static routes on page 21
- Configuring DNS on page 22
- Capturing voice and fax packets on page 23

Configuring the network interfaces

The *System > Network > Network* tab displays the FortiVoice Gateway's network interfaces.

You must configure at least one network interface for the FortiVoice Gateway to connect to your network. Depending on your network topology and other considerations, you can connect the FortiVoice Gateway to your network using two or more of the network interfaces. You can configure each network interface separately. You can also configure advanced interface options, including VLAN subinterfaces, redundant interfaces, and loopback interfaces. For more information, see About FortiVoice Gateway logical interfaces on page 17 and Creating or editing network interfaces on page 19.

To view the list of network interfaces, go to *System > Network > Network*.

GUI field	Description
Name	Displays the name of the network interface, such as *port1*
Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see About FortiVoice Gateway logical interfaces on page 17.
IP/Netmask	Displays the IP address and netmask of the network interface.
IPv6/Netmask	Displays the IPv6 address and netmask of the network interface.
Access	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the GUI.
Status	Indicates the **up** (available) or **down** (unavailable) administrative status for the network interface. • *Green check mark*: The network interface is up and can receive traffic. • *Red check mark*: The network interface is down and cannot receive traffic. To change the administrative status (bring up or down a network interface), see Creating or editing network interfaces on page 19.
References (icon)	Indicates if a network interface is used by other services, such as DHCP. A green dot means a network interface is used by other services. A gray dot means a network interface is not used by other services.

Creating or editing network interfaces

You can edit FortiVoice Gateway's physical network interfaces to change its IP addresses, netmasks, administrative access protocols, and other settings. You can also create or edit logical interfaces, such as VLANs, redundant interfaces and the loopback interface.

> ⚠️ Enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiVoice Gateway.

You can restrict which IP addresses are permitted to log in as a FortiVoice Gateway administrator through network interfaces. For details, see Configuring administrator accounts on page 24.

To create or edit a network interface

1. Go to *System > Network > Network*.
2. Double-click a network interface to modify it or select the interface and click *Edit*. If you want to create a logical interface, click *New*.
   The *Interface* dialog appears.
3. Configure the following:

GUI field	Description
Interface name	If you are editing an existing interface, this field displays the name (such as port2) and media access control (MAC) address for this network interface.

GUI field	Description
	If you are creating a logical interface, enter a name for the interface.
Type	If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see About FortiVoice Gateway logical interfaces on page 17. • *VLAN*: If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface. • Specify an *Interface* (port) and *VLAN ID*. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved. • *Redundant*: If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members. • *Loopback*: If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to "loopback". You can only add one loopback interface on the FortiVoice Gateway.
Addressing Mode	• *Manual*: Select to enter the IP address or IPv6 address and netmask for the network interface in *IP/Netmask* or *IPv6/Netmask*. • *DHCP*: Select and click *Update Request* to retrieve a dynamic IP address using DHCP.
Advanced Setting	Enable protocols that this network interface should accept for connections **to** the FortiVoice Gateway itself. (These options do not affect connections that will travel **through** the FortiVoice Gateway.) ⚠ HTTP and Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiVoice Gateway. For information on further restricting access of administrative connections, see Configuring administrator accounts on page 24. • *HTTPS*: Enable to allow secure HTTPS connections to the web-based manager, and extension user account through this network interface. • *SNMP*: Enable to allow SNMP connections (queries) to this network interface. For information on further restricting access, or on configuring the network interface that will be the source of traps, see Configuring the network interfaces on page 18. • *TFTP*: Enable to allow TFTP connections to the CLI through this network interface. The SIP phones connect to this server to receive the PBX setup information. • *SIPPNP*: Enable SIPPNP multicast function for the connected phones to find the provisioning server contained in its message for the phones. • *PING*: Enable to allow ICMP ECHO (ping) responses from this network interface. • *HTTP*: Enable to allow HTTP connections to the web-based manager, and extension user account through this network interface. • *NTP:* Enable to allow SIP phones to connect to this server to synchronize time. • *MDNS*: Enable MDNS multicast function for the connected phones to find the TFTP

GUI field	Description
	provisioning server contained in its message for the phones. This is mainly for backward support of legacy FortiFones. • *SSH*: Enable to allow SSH connections to the CLI through this network interface. • *TELNET*: Enable to allow Telnet connections to the CLI through this network interface. • *LDAP*: Enable to allow SIP phones to connect to this server to retrieve phone directories.

	• *MTU:* You can change the maximum transmission unit (MTU) value which represents the maximum packet or Ethernet frame size in bytes.
	If network devices between the FortiVoice Gateway and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance.
	The default value is 1500 bytes.
	The MTU size must be between 68 and 9000 bytes.
	• *Administrative status*: Select either:
	   • *Up*: Enable (bring up) the network interface so that it can send and receive traffic.
	   • *Down*: Disable (bring down) the network interface so that it cannot send or receive traffic.

4. Click *Create* or *OK*.

Configuring static routes

The *System > Network > Routing* tab displays a list of routes and lets you configure static routes and gateways used by the FortiVoice Gateway.

Static routes direct traffic exiting the FortiVoice Gateway. You can specify through which network interface a packet will leave, and the IP address of a next-hop router that is reachable from that network interface. The router is aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations.

A default route is a special type of static route. A default route matches all packets, and defines a gateway router that can receive and route packets if no other, more specific static route is defined for the packet's destination IP address.

Configure at least one static route, a default route, that points to your gateway. If you have multiple gateway routers, each of which should receive packets destined for a different subset of IP addresses, configure multiple static routes.

To determine which route a packet will be subject to, the FortiVoice Gateway compares the packet's destination IP address to those of the static routes and forwards the packet to the route with the large prefix match.

When you add a static route through the GUI, the FortiVoice Gateway evaluates the route to determine if it represents a different route compared to any other route already present in the list of static routes. If no route having the same destination exists in the list of static routes, the FortiVoice Gateway adds the static route.

To view or configure static routes

1. Go to *System > Network > Routing*.

GUI field	Description
Enabled	Displays the route status.
Destination IP/Netmask	Displays the destination IP address and subnet of packets subject to the static route. A setting of `0.0.0.0/0.0.0.0` indicates that the route matches all destination IP addresses.
Gateway	Displays the IP address of the next-hop router to which packets subject to the static route will be forwarded.
Interface	The interface that this route applies to.
Comment	Displays any notes on the static route.

2. Either click *New* to add a route or double-click a route to modify it.
   A Routing Entry dialog appears.
3. Select *Enable* to activate the static route.
4. In *Destination IP/netmask*, enter the destination IP address and netmask of packets that will be subject to this static route.
   To create a default route that will match all packets, enter `0.0.0.0/0.0.0.0`.
5. Select the interface that this route applies to.
6. In *Gateway*, type the IP address of the next-hop router to which the FortiVoice Gateway will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in *Destination IP/netmask*. For an Internet connection, the next hop routing gateway routes traffic to the Internet.
7. In *Comments*, enter any notes you have for the route.
8. Click *Create* or *OK*.

Configuring DNS

FortiVoice Gateway units require Domain Name System (DNS) servers for features such as reverse DNS lookups. Your ISP may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers.

> For improved FortiVoice Gateway performance, use DNS servers on your local network.

The *System > Network > DNS* tab lets you configure the DNS servers that the FortiVoice Gateway queries to resolve domain names into IP addresses.

To configure the primary and secondary DNS servers

1. Go to *System > Network > DNS*.
2. In *Primary DNS server*, enter the IP address of the primary DNS server.

3. In *Secondary DNS server*, enter the IP address of the secondary DNS server.
4. Click *Apply*.

Capturing voice and fax packets

When troubleshooting networks, it helps to look inside the contents of the packets. This helps to determine if the packets, route, and destination are all what you expect. Traffic capture can also be called packet sniffing, a network tap, or logic analyzing.

Packet sniffing tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- Finding missing traffic.
- Seeing if sessions are setting up properly.
- Locating ARP problems, such as broadcast storm sources and causes.
- Confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks.
- Confirming routing is working as expected.
- Intermittent missing PING packets.

If you are running a constant traffic application, such as ping, packet sniffing can tell you if the traffic is reaching the destination, how the port enters and exits the FortiVoice Gateway, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start sniffing packets, you need to have a good idea of what you are looking for. Sniffing is used to confirm or deny your ideas about what is happening on the network. If you try sniffing without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to sniff enough packets to really understand all of the patterns and behavior that you are looking for.

To capture voice and fax packets

1. Go to *System > Network > Traffic Capture*.

Button or GUI field	Description
Stop	Click to stop the packet capture.
Download	When the capture is complete, click *Download* to save the packet capture file to your hard disk for further analysis.
Name	The name of the packet capture file.
Size	The size (byte) of the packet capture file.
Status	The status of the packet capture process, *Complete* or *Running*.

2. Click *New*.
3. In *Capture file prefix*, enter a prefix for the file generated from the captured traffic. This will make it easier to recognize the files.
4. In *Duration*, enter the time period for performing the packet capture.
5. If you choose *SIP* or *Use protocol* for *Filter*, from the *Peers* field, select the extension or trunk to capture the voice packets. You can select up to three peers.

6. If you want to limit the scope of traffic capture, in the *IP/Host* field, enter a maximum of three IP addresses or host names for the extensions and trunks you selected. Only traffic on these IP addresses or host names is captured.

7. Select the filter for the traffic capture:
    - *SIP*: Only SIP traffic of the peers you select will be captured.
    - *Use Protocol*: Only UDP or TCP traffic of the peers you select will be captured.
    - *Capture All*: All network traffic will be captured.

8. For *Exclusion*, enter the IP addresses/host names and port numbers of which you do not want to capture voice traffic.

9. Click *Create*.

Configuring administrator accounts

The *System > Administrator > Administrator* tab displays a list of the FortiVoice Gateway's administrator accounts and the trusted host IP addresses administrators use to log in (if configured).

By default, FortiVoice Gateway has a single administrator account, `admin`.

Prerequisite

If you want to create or edit an admin profile, perform this task on the FortiVoice phone system first. For more details about the admin profile, see the Configuring administrator profiles section in the FortiVoice Phone System Administration Guide.

To view administrator accounts, go to *System > Administrator > Administrator*. The following table includes the GUI fields and descriptions.

GUI field	Description
Enabled	Displays the administrator status.
Name	Displays the name for this administrator account.
Admin profile	The administrator profile that determines which functional areas the administrator account can view or affect.
Authentication Type	The administrator authentication type: Local, RADIUS, LDAP, or Single Sign On.
Authentication Profile	The LDAP authentication profile.
Trusted Hosts	Displays the IP address and netmask from which the administrator can log in.

To configure administrator accounts

1. Go to *System > Administrator > Administrator*.
2. Click *New* to add an account.
    An Administrator dialog appears.
3. Configure the following fields:

GUI field	Description
Enabled	Click to activate the administrator status. By default, this is enabled.
Administrator	Enter the name for this administrator account.

GUI field	Description
	The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.
Email address	Enter the administrator's email address.
Admin profile	Select the name of an admin profile that determines which functional areas the administrator account can view or affect.
Authentication type	Select an administrator authentication type: *Local*, *RADIUS*, *LDAP*, or *Single Sign On*.
New password	This field does not appear if *Authentication type* is *LDAP*. Enter the password for this account. The password can contain any character except spaces. ⚠️ Enter a FortiVoice administrator password that has six characters or more. For better security, enter a password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiVoice Gateway unit.
Confirm password	Enter the account password again to confirm it.
RADIUS profile	If you select *RADIUS* for *Authentication Type*, select a RADIUS authentication profile. If you want to create a new RADIUS profile, click +.
LDAP profile	If you select *LDAP* for *Authentication Type*, select an LDAP authentication profile.
Trusted hosts type	Select a trusted host type: • *User defined*: Add details about the hosts in *Trusted Hosts*. • *RFC 1918 predefined*: The FortiVoice Gateway unit allows connections from any private IP addresses specified by the request for comment 1918 (RFC 1918).
Trusted hosts	Enter an IPv4 or IPv6 address or subnet from which this administrator can log in. If you want the administrator to access the FortiVoice Gateway unit from any IP address, use `0.0.0.0/0.0.0.0`. Enter the IP address and netmask in dotted decimal format. For example, you might permit the administrator to log in to the FortiVoice Gateway unit from your private network by typing `192.168.1.0/255.255.255.0`.

GUI field	Description
	For additional security, restrict all trusted host entries to administrative hosts on your trusted private network. For example, if your FortiVoice administrators log in only from the 10.10.10.10/24 subnet, to prevent possibly fraudulent login attempts from unauthorized locations, you could configure that subnet in the *Trusted Host #1*, *Trusted Host #2*, and *Trusted Host #3* fields.
	For information about restricting administrative access protocols that can be used by these hosts, see Creating or editing network interfaces on page 19. Click the + sign to add additional IP addresses or subnets from which the administrator can log in.
Select language	Select this administrator account's preference for the display language of the GUI.
Select theme	Select this administrator account's preference for the display theme or click *Use Current* to choose the theme currently in effect. The administrator may switch the theme at any time during a session by clicking *Next Theme*.
Description	Select *Click to edit* to enter any comments for the administrator account.

4. Click *Create*.

Configuring system time, system options, SNMP queries and traps, email setting, and GUI appearance

The *System > Configuration* menu lets you configure the system time, system options, SNMP queries and traps, email setting, and GUI appearance.

This topic includes:

- Configuring the time and date on page 26
- Configuring system options on page 27
- Configuring SNMP queries and traps on page 28
- Configuring email settings on page 34
- Customizing the GUI appearance on page 35

Configuring the time and date

The *System > Configuration > Time* tab lets you configure the system time and date of the FortiVoice Gateway.

You can either manually set the FortiVoice Gateway system time or configure the FortiVoice Gateway to automatically keep its system time correct by synchronizing with Network Time Protocol (NTP) servers.

> For many features to work, including scheduling, logging, and certificate-dependent features, the FortiVoice Gateway system time must be accurate.
> FortiVoice Gateway supports daylight savings time (DST).

To configure the system time

1. Go to *System > Configuration > Time*.
2. Configure the following:

GUI field	Description
System time	Displays the date and time according to the FortiVoice Gateway's clock at the time that this tab was loaded, or when you last selected the *Refresh* button.
Time zone	Select the time zone in which the FortiVoice Gateway is located. *Automatically adjust clock for daylight saving time changes*: Enable to adjust the FortiVoice Gateway system clock automatically when your time zone changes to daylight savings time (DST) and back to standard time.
Set Date	Select this option to manually set the date and time of the FortiVoice Gateway's clock, then select the *Year*, *Month*, *Day,Hour*, *Minute*, and *Second* fields before you click *Apply*. Alternatively, configure *Synchronize with NTP server*.
Synchronize with NTP Server	Select to use a network time protocol (NTP) server to automatically set the system date and time, then configure *Server* and *Sync Interval*. • *Server*: Enter the IP address or domain name of an NTP server. You can add a maximum of 10 NTP servers. The FortiVoice Gateway uses the first NTP server based on the selection mechanism of the NTP protocol. Click the + sign to add more servers. Click the - sign to remove servers. Note that you cannot remove the last server. To find the NTP servers that you can use, see http://www.ntp.org. • *Sync interval*: Enter how often, in minutes, the FortiVoice Gateway should synchronize its time with the NTP server. For example, entering 1440 causes the FortiVoice Gateway to synchronize its time once a day. Depending on your network traffic, it may take some time for the FortiVoice Gateway to synchronize its time with the NTP server.

3. Click *Apply*.

Configuring system options

The *System > Configuration > Option* tab lets you set the following global settings:

- system idle timeout
- administration ports on the interfaces

To view and configure the system options

1. Go to *System > Configuration > Option*.
2. Configure the following:

GUI field	Description
Idle timeout	Enter the amount of time that an administrator may be inactive before the FortiVoice Gateway automatically logs out the administrator. For better security, use a low idle timeout value.
Administration Ports	Specify the TCP ports for administrative access on all interfaces. Default port numbers: HTTP: 80 HTTPS: 443 SSH: 22 TELNET: 23

3. Click *Apply*.

Configuring SNMP queries and traps

Go to *System > Configuration > SNMP* to configure SNMP to monitor FortiVoice Gateway events and thresholds.

To monitor FortiVoice Gateway information and receive FortiVoice traps, you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager. RFC support includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). For more information, see FortiVoice MIBs on page 32.

The FortiVoice SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiVoice Gateway information and can receive FortiVoice traps.

The FortiVoice SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Before you can use its SNMP queries, you must enable SNMP access on the network interfaces that SNMP managers will use to access the FortiVoice Gateway. For more information, see Creating or editing network interfaces on page 19.

This topic includes:

- Configuring an SNMP threshold on page 28
- Configuring an SNMP v1 and v2c community on page 30
- Configuring an SNMP v3 user on page 31
- FortiVoice MIBs on page 32
- FortiVoice traps on page 33

Configuring an SNMP threshold

Configure under what circumstances an event is triggered.

To set SNMP thresholds

1. Go to *System > Configuration > SNMP*.
2. Configure the following:

GUI field	Description
SNMP agent enabled	Enable to activate the FortiVoice SNMP agent. This must be enabled to accept queries from SNMP managers or send traps from the FortiVoice Gateway.
Description	Enter a descriptive name for the FortiVoice Gateway .
Location	Enter the location of the FortiVoice Gateway .
Contact	Enter administrator contact information.
SNMP Threshold	To change a value in the four editable columns, select the value in any row. It becomes editable. Change the value and click outside of the field. A red triangle appears in the field's corner and remains until you click *Apply*.
Trap Type	Displays the type of trap, such as *CPU Usage*.
Trigger	You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered. For example, using the default value, if the mailbox disk is 90% or more full, it will trigger.
Threshold	Sets the number of triggers that will result in an SNMP trap. For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one, an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period.
Sample Period (s)	Sets the time period in seconds during which the FortiVoice Gateway SNMP agent counts the number of triggers that occurred. This value should **not** be less than the *Sample Freq(s)* value.
Sample Freq(s)	Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period. This value should be less than the *Sample Period(s)* value.
Community	Displays the list of SNMP communities (for SNMP v1 and v2c) added to the FortiVoice configuration. For information on configuring a community, see either Configuring an SNMP v1 and v2c community on page 30 or Configuring an SNMP v3 user on page 31.
Enabled	Displays the status of the SNMP community and allows you to change it.
Name	Displays the name of the SNMP community. The SNMP Manager must be configured with this name.
Queries	A green check mark icon indicates that queries are enabled.
Traps	A green check mark icon indicates that traps are enabled.
User	Displays the list of SNMP v3 users added to the FortiVoice configuration. For information on configuring a v3 user, see Configuring an SNMP v3 user on page 31.
Enabled	Displays the status of the SNMP v3 user and allows you to change it.

GUI field	Description
Name	Displays the name of the SNMP v3 user. The SNMP Manager must be configured with this name.
Queries	A green check mark icon indicates that queries are enabled.
Traps	A green check mark icon indicates that traps are enabled.
Security Level	Displays the security level.

3. Click *Apply*.

Configuring an SNMP v1 and v2c community

An SNMP community is a grouping of equipment for SNMP-based network administration purposes. You can add up to three SNMP communities so that SNMP managers can connect to the FortiVoice Gateway to view system information and receive SNMP traps. You can configure each community differently for SNMP traps and to monitor different events. You can add the IP addresses of up to eight SNMP managers to each community.

To configure an SNMP community

1. Go to *System > Configuration > SNMP*.
2. Under *Community*, click *New* to add a community or select a community and click *Edit*.
   The *SNMP Community* page appears.
3. Configure the following:

GUI field	Description
Enabled	Enable to send traps to and allow queries from the community's SNMP managers.
Name	Enter a name to identify the SNMP community. If you are editing an existing community, you cannot change the name. You can add up to 16 communities.
Community Hosts	Lists SNMP managers that can use the Setting in this SNMP community to monitor the FortiVoice Gateway . Click *Create* to create a new entry. You can add up to 16 hosts.
IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP community.
Create (button)	Click to add a new default entry to the *Hosts* list that you can edit as needed.
Delete (button)	Click to remove this SNMP manager.
Queries	Enter the *Port* number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiVoice Gateway . Mark the *Enable* check box to activate queries for each SNMP version.

GUI field	Description
Traps	Enter the *Local Port* and *Remote Port* numbers (162 local, 162 remote by default) that the FortiVoice Gateway uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Enable traps for each SNMP version that the SNMP managers use. Enable each SNMP event for which the FortiVoice Gateway should send traps to the SNMP managers in this community.
	Not all events will trigger traps because FortiVoice Gateway checks its status in a scheduled interval. For example, FortiVoice Gateway checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.

4. Click *Create*.

Configuring an SNMP v3 user

SNMP v3 adds more security by using authentication and privacy encryption. You can specify an SNMP v3 user on FortiVoice so that SNMP managers can connect to the FortiVoice Gateway to view system information and receive SNMP traps.

To configure an SNMP v3 user

1. Go to *System > Configuration > SNMP*.
2. Under *User*, click *New* to add a user or select a user and click *Edit*.
   The *SNMPv3 User* page appears.
   You can add up to 16 users.
3. Configure the following:

GUI field	Description
Enabled	Enable to send traps to and allow queries from the user's SNMP managers.
User name	Enter a name to identify the SNMP user. If you are editing an existing user, you cannot change the name.
Security level	Choose one of the three security levels: • *No authentication, no privacy*: This option is similar to SNMP v1 and v2. • *Authentication, no privacy*: This option enables authentication only. The SNMP manager needs to supply a password that matches the password you specify on FortiVoice. You must also specify the authentication protocol (either SHA1 or MD5). • *Authentication, privacy*: This option enables both authentication and encryption. You must specify the protocols and passwords. Both the protocols and passwords on the SNMP manager and FortiVoice must match.

GUI field	Description
Authentication Protocol	For *Security level*, if you select either *Authentication* option, you must specify the authentication protocol and password. Both the authentication protocol and password on the SNMP manager and FortiVoice must match.
Privacy protocol	For *Security level*, if you select *Privacy,* you must specify the encryption protocol and password. Both the encryption protocol and password on the SNMP manager and FortiVoice must match.
Notification Hosts	Lists the SNMP managers that FortiVoice will send traps to. Click *Create* to create a new entry. You can add up to 16 host.
IP Address (button)	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP user.
Create (button)	Click to add a new default entry to the *Hosts* list that you can edit as needed.
Delete (button)	Click to remove this SNMP manager.
Queries	Double click the default port number (161) to enter the *Port* number that the SNMP managers use for SNMP v3 queries to receive configuration information from the FortiVoice Gateway . Select the *Enable* check box to activate queries.
Traps	Double click the default local port (162) and remote port number (162) to enter the *Local Port* and *Remote Port* numbers that the FortiVoice Gateway uses to send SNMP v3 traps to the SNMP managers. Select the *Enable* check box to activate traps. Enable each SNMP event for which the FortiVoice Gateway should send traps to the SNMP managers. Not all events trigger traps because the FortiVoice Gateway checks its status at a scheduled interval. For example, FortiVoice checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.

4. Click *Create*.

FortiVoice MIBs

The FortiVoice SNMP agent supports Fortinet proprietary Management Information Base (MIB) as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiVoice Gateway configuration.

The FortiVoice MIBs are listed in FortiVoice MIBs on page 33. You can obtain these MIB files from Fortinet technical support. To communicate with the SNMP agent, you must compile these MIBs into your SNMP manager.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

FortiVoice MIBs

MIB file name	Description
FortiVoice.mib	Displays the proprietary Fortinet MIB includes detailed FortiVoice Gateway configuration information. Your SNMP manager requires this information to monitor FortiVoice configuration Setting. For more information, see MIB fields on page 33.

FortiVoice traps

The FortiVoice Gateway's SNMP agent can send traps to SNMP managers that you have added to SNMP communities. To receive traps, you must load and compile the FortiVoice trap MIB into the SNMP manager.

All traps sent include the trap message as well as the FortiVoice Gateway serial number and host name.

MIB fields

Trap	Description
fvTrapStorageDiskHighThreshold	Trap sent if log disk usage and mailbox disk usage become too high.
fvTrapSystemEvent	Trap sent when the system performs actions such as shutting down, rebooting, and upgrading.
fmlTrapHAEvent	Trap sent when an HA event occurs.

The Fortinet MIB contains fields reporting current FortiVoice Gateway status information. The tables below list the names of the MIB fields and describe the status information available for each. You can view more details about the information available from all Fortinet MIB fields by compiling the MIB file into your SNMP manager and browsing the MIB fields.

System session MIB fields

MIB field	Description
fvSysModel	FortiVoice Gateway model number.
fvSysSerial	FortiVoice Gateway serial number.
fvSysVersion	The firmware version currently running on the FortiVoice Gateway .
fvSysCpuUsage	The current CPU usage (%).
fvSysMemUsage	The current memory utilization (%).
fvSysLogDiskUsage	The log disk usage (%).
fvSysStorageDiskUsage	The storage disk usage (%).
fvSysEventCode	System component events.
fvSysload	Current system load.

Configuring email settings

You can configure the FortiVoice Gateway to send email notifications to phone users when they miss a phone call or receive a voicemail or fax.

> For phone users to receive the notifications, you need to add their email addresses when configuring the extensions.

To configure email settings

1. Go to *System > Configuration > Mail Setting*.
2. Configure the following fields:

GUI field		Description
Local Host		
	Host name	Enter the host name of the FortiVoice Gateway, such as `FortiVoice Gateway GT02.`
	Local domain name	Enter the local domain name of the FortiVoice Gateway, such as `example.com.`
Mail Queue		
	Maximum time for email in queue (1-240 hours)	Enter the maximum number of hours that deferred email messages can remain in the deferred email queue, during which the FortiVoice Gateway periodically retries to send the message. After it reaches the maximum time, the FortiVoice Gateway sends a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable.
	Time interval for retry (10-120 minutes)	Enter the number of minutes between delivery retries for email messages in the deferred mail queues.
Relay Server		Configure an SMTP relay, if needed, to which the FortiVoice Gateway will relay outgoing email. This is typically provided by your Internet service provider (ISP), but could be a mail relay on your internal network.
	Relay server name	Enter the domain name of an SMTP relay.
	Relay server port	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).
	Use SMTPs	Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiVoice Gateway built-in MTA (or proxy) to the relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPs connections.

GUI field	Description

Authentication required	Select the checkbox and click the arrow to expand the section and configure:
	• *User name*: Enter the name of the FortiVoice Gateway account on the SMTP relay.
	• *Password*: Enter the password for the FortiVoice Gateway user name.
	• *Authentication type*: Available SMTP authentication types include:
	  • *AUTO* (automatically detects and uses the most secure SMTP authentication type supported by the relay server)
	  • *LOGIN* (provides an unencrypted, scrambled password)
	  • *PLAIN* (provides an unencrypted, scrambled password)
	  • *CRAM-MD5* (provides an encrypted hash of the password, with hash replay prevention, combined with a challenge and response mechanism)
	  • *DIGEST-MD5* (provides an encrypted hash of the password)

Test (button)	After you have entered the relay server information, you can test if the relay server is accessible: 1. Click the *Test* button. 2. To further test the mail delivery, click *Advanced Group*, and enter the sender (MAIL FROM) and recipient (RCPT TO) email addresses. The EHLO (Extended HELO) information is filled in by default. 3. To start the test and display the test results, click the *Test* button.

3. Click *Apply*.

Customizing the GUI appearance

The *System > Configuration > Appearance* tab lets you customize the default appearance of the web-based manager and voicemail interface with your own product name, product icon, corporate logo, and language.

To customize the GUI appearance

1. Go to *System > Configuration > Appearance*.
2. Configure the following fields:

GUI field	Description
Product name	Enter the name of the product. This name will precede *Administrator Login* in the title on the login page of the GUI.
Product icon	To browse and upload an image that will appear on the browser tab, click *Change*. The image must meet the following requirements:

GUI field	Description
	• Supported image file format: ICO • Image dimensions must be 16 x 16 pixels. To return to the default setting, click *Reset*.
Top logo	To browse and upload an image that will appear at the top of all pages in the GUI, click *Change*. The image must meed the following requirements: • Supported image file formats: JPEG and PNG • Image dimensions must be 460 x 36 pixels. For best results, use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic. ⚠️ The FortiVoice Gateway does not save a backup copy of your image. Make sure to save a backup copy of the image on your management computer to allow you to upload an image again at a later time, if necessary. To return to the default setting, click *Reset*.
Default UI language	Select the default language for the display of the web-based manager. You can configure a separate language preference for each administrator account. For details, see Configuring administrator accounts on page 24.
Default theme	Select the default color for the web-based manager GUI.

3. Click *Apply*.
4. If you have changed the product icon or top logo, or both, clean the browser history and refresh the browser window to see the updated icon.

Configuring advanced system settings

The *System > Advanced Setting* submenu lets you configure the FortiVoice Gateway location, SIP setting, and notification email templates.

This topic includes:

- Configuring FortiVoice Gateway location and contact information on page 36
- Configuring SIP settings on page 37
- Customizing notification email templates on page 38

Configuring FortiVoice Gateway location and contact information

Identify the FortiVoice Gateway location and its number.

To set the location

1. Go to *System > Advanced Setting > Location*.
2. Configure the following fields:

GUI field	Description
Country/Region	Select the country where the FortiVoice Gateway is in.
Emergency number	Click the default number (911) to enter the emergency call number of the selected country.
Long-distance prefix	To edit the prefix for dialing long-distance calls, click ✎.
International prefix	To edit the prefix for dialing international calls, click ✎.
Outside line prefix	To edit the prefix for making outbound calls, click ✎.
Area code	To enter the *Area code* for the main number of the FortiVoice Gateway, click ✎. Ask your PSTN service provider for this code.
Required when dialing local numbers	Select this option if the area code needs to be dialed for local phone calls.
Main display name	Enter the name displaying on the FortiVoice Gateway. Ask your PSTN service provider for this name.
Main number	Enter the main number of the FortiVoice Gateway. Ask your PSTN service provider for this number.
Default prompt language	Select a new default prompt language for the FortiVoice Gateway. The default is English. To add a prompt language, click *New*. In the *Upload* field, click *Browse* to upload the language file provided by Fortinet Support. Click *OK*.
Default emergency zone	Select the default emergency contact or click + to add a new one.
Default time zone	Select a new default time zone for the FortiVoice Gateway.

3. Click *Apply*.

Configuring SIP settings

The FortiVoice Gateway supports SIP communications.

To configure SIP settings

1. Go to *System > Advanced Setting > SIP*.
2. Configure the following fields:

GUI field	Description
SIP Transport and Internal Ports	Enable and enter the ports, as required.

GUI field		Description
		SIP communication commonly uses TCP or UDP port 5060 and/or 5061.
		Port 5060 is used for nonencrypted SIP signaling sessions.
		Port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS).
		The WebSocket Secure (WSS) protocol establishes a WebSocket over an encrypted TLS connection. The default port is 8089.
RTP Setting		
	Port	Enter the start and end RTP ports that the FortiVoice Gateway will use for phone call sessions.
		Make sure that there is a reasonable port range so that you have enough ports for all open calls. The default port range is 10000 to 30000.
	Timeout	Enter the amount of time in seconds during an active call that the extension will wait for RTP packets before hanging up the call. A value of 0 (zero) means there is no time limit. The default is 7200.
	Hold timeout	Enter the amount of time in seconds that the extension will wait on hold for RTP packets before hanging up the call. A value of 0 (zero) means there is no time limit. The default is 7200.

3. Click *Apply*.

Customizing notification email templates

Go to *System > Advanced Setting > Custom Message* to view and reword the default notification email templates. The FortiVoice Gateway sends out notification email when, for example, you have a new voicemail or fax in your mailbox or missed a call. You can customize the email templates for the email notifications. You can change the content of the email template by editing the text and HTML codes and by working with email template variables. For descriptions of the default email template variables, select a template and click *Edit Variable*.

To customize email templates

1. Go to *System > Advanced Setting > Custom Message*.
2. Open *Email template* to display the default templates.
3. To edit a template, double-click it or select it and click *Edit*.
4. To format template in HTML, use HTML tags, such as `<b>some bold text</b>`.
   There is a limit of 250 characters for the *Subject* field, 60 characters for the *From* field, and 4000 characters for *Htmlbody* and *Textbody* messages each in the *Content* body field.
5. To add a variable:
   - Select *Insert Variables* next to the area to insert a variable. A pop-up window appears.
   - Place your mouse cursor in the text message at the insertion point for the variable.
   - Click the name of the variable to add. It appears at the insertion point.
   - To add another variable, click the message area first, then click the variable name.
   - Click the *Close (X)* icon to close the window.

- To insert a color:
  - Click *Insert Color Code*. A pop-up window of color selection appears.
  - Place your mouse cursor in the text at the insertion point for the color code, or highlight an existing color code to change.
  - Click a color in the color selection pop-up window.

  For example, to replace the color code in the HTML tag `<tr bgcolor="#3366ff">`, you can highlight `"#3366ff"`, then select the color you want from the color palette.

  To add a new color code, include it with HTML tags as applicable, such as `<tr bgcolor="#3366ff">`.

6. To determine if your HTML and color changes are correct, click *Preview*. The replacement message appears in HTML format.
7. Click *OK*, or click *Reset To Default* to revert the replacement message to its default text.

Maintaining the system

The *System > Maintenance* submenu allows you to perform scheduled maintenance.

This topic includes:

- Backing up the configuration on page 39
- Downloading a trace log file on page 40
- Restoring the configuration on page 40
- Restoring the firmware on page 40

Backing up the configuration

Before installing the FortiVoice Gateway firmware or making significant configuration changes, back up your FortiVoice Gateway configuration. Backups let you revert to your previous configuration if the new configuration does not function correctly. Backups let you compare changes in configuration.

You can back up system configuration or user configuration. System configuration includes the configurations that make the FortiVoice Gateway work. User configuration includes user-configured settings, such as voicemail greetings, in addition to system configuration.

In addition to backing up your configuration manually, you can also configure a schedule to back up the configuration automatically to the FortiVoice Gateway local hard drive or a remote FTP/SFTP server.

To back up the configuration file

1. Go to *System > Maintenance > Configuration*.
2. In the *Backup* area, select *System configuration* or *User data*.
   If you choose to back up user data and the user data files are not updated, select the files to be updated and click *Prepare* first before proceeding to the next step.
3. Click *Backup*.
   Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection. You can restore the backup configuration later when required. For details, see Restoring the configuration on page 40.

To schedule a configuration backup

1. Go to *System > Maintenance > Configuration*.
2. Under *Scheduled Backup*, configure the schedule time and the maximum backup number. When the maximum number is reached, the oldest version will be overwritten.
3. If you want to back up locally, enable *Local Backup*.
4. If you want to back up remotely, enable *Remote backup* and configure the FTP or SFTP server credentials.
5. Click *Apply*.

Downloading a trace log file

If Fortinet Support requests a trace log for system analysis purposes, you can download one using the GUI.

Trace logs contain information that is supplementary to debug-level log files.

To download a trace log file

1. Go to *System > Maintenance > Configuration > Trace Log*.
2. Configure *Trace Log* settings.
3. Click *Prepare* to make the trace log file ready before downloading it.
4. Click *Refresh*.
5. Click *Download trace log*.
6. Save the file on your local PC.
7. Send the file to Fortinet Support.

Restoring the configuration

1. To restore the backup FortiVoice Gateway configuration from your local PC, go to *System > Maintenance > Configuration > Restore Configuration*.
2. Click *Browse* to locate and select the configuration file that you want to restore.
3. Click *Open*.
4. To confirm, click *Yes*.
    The FortiVoice Gateway restores the configuration file and reboots. The required time varies by the file size and the speed of your network connection.
5. Verify the configuration restoration:
    a. Clear your browser's cache and refresh the login page of the GUI.
    b. Log in to the GUI using the admin administrator account.
    c. Review the configuration and verify that the configuration has been correctly restored.

Restoring the firmware

1. To restore a FortiVoice Gateway firmware from your local PC, go to *System > Maintenance > Configuration > Restore Firmware*.
2. Click *Browse* to locate and select the firmware.
3. Click *Open*.

4. To confirm, click *Yes*.
   The FortiVoice Gateway restores the firmware file and reboots. The required time varies by the file size and the speed of your network connection.
5. Verify the firmware restoration:
   a. Clear your browser's cache and refresh the login page of the GUI.
   b. Log in to the GUI using the admin administrator account.
   c. Review the configuration and verify that the firmware has been correctly restored.

Configuring the FortiVoice Gateway

Configure the FortiVoice Gateway to connect your voice and data to the outside world.

This section includes the following topics:

Creating SIP peer for IP-PBX

You can add one or more VoIP service providers to the FortiVoice Gateway trunk configuration. The VoIP service providers deliver your telephone services to customers equipped with SIP-based PBX (IP-PBX).

To view the list of VoIP service providers, go to *Gateway > SIP > SIP*. The following table includes the GUI fields and descriptions.

GUI field	Description
Test	Select to test if the trunk is created successfully. For more information, see Testing SIP trunks on page 46.
FortiCall	Select to create a SIP trunk with Fortinet's FortiCall service. You can only create one trunk with FortiCall and use it free for 30 days or 300 minutes, whichever comes first. Note that the trial account only allows outbound calling and no international calling is available. If you sign up for the service during a trial, the trial is closed and billing will start. For more information, see Creating a SIP trunk with FortiCall service on page 46.
Enabled	Select to activate this trunk.
Name	The name of the VoIP service provider.
Server	The VoIP provider's domain name or IP address. For example, `172.20.120.11` or `voip.example.com`.
Port	The port for SIP sessions.
SIP Setting	The SIP profile applied to this trunk.
Status	The status of the SIP trunk. • *Not registered*: The trunk is not registered with the VoIP service provider and is not in service. • *In service*: The trunk is registered with the VoIP service provider and is in service.

GUI field	Description
	• *Unavailable*: The trunk is not reachable. • *Alarm detected*: There is a problem with the phone line. • *Admin down*: The trunk is disabled. • *Unmonitored*: The trunk is unknown.

To create a VoIP trunk

1. Go to *Gateway > SIP > SIP*.
2. Click *New*.
3. Configure the following:

GUI field		Description
Enabled		Select to activate this trunk.
Name		Enter the name of the VoIP service provider.
Display name		Enter your caller ID that will appear on the called phone, such as Example Company.
Main number		Enter the phone number that will appear on the called phone.
SIP Setting		
	SIP server	Enter the VoIP provider's IP address or domain name. For example, `172.20.120.11` or `voip.example.com`.
	SIP port	Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number. If you select the *Using DNS record* option, this field is greyed out.
	Using SRV record	If you entered the VoIP provider's domain name in the *SIP server* field, select this option to translate the domain name and obtain the SIP port. You can only select this option if your VoIP provider uses the same setting.
	User name	Enter the user name provided by the VoIP service provider for the FortiVoice Gateway to register with the SIP server.
	Password	Enter the password provided by the VoIP service provider for the FortiVoice Gateway to register with the SIP server.
	Auth. user name	Some VoIP providers may provide you with an authentication user name that is different from your user name for the FortiVoice Gateway to register with the SIP server. If that is the case, enter the authentication user name here.

GUI field		Description
	Realm/domain	Some VoIP service providers' SIP servers authenticate the PBXs that register with them by requesting the name of the host performing the authentication. If this is the case with your VoIP service provider, enter the name of the host performing the authentication provided by your VoIP service provider.
	SIP settings	Select the SIP profile to apply the supported phone features and codecs for the trunk. To match the information of the VoIP service provider, you can edit the existing profile or click *New* to add a new one. For more information, see Configuring SIP profiles on page 47.
	Max channel	Each trunk contains multiple channels. The number of channels you can have in a trunk is controlled by your VoIP service provider. Consult your VoIP service provider for the maximum of channels that you can set to limit the number of concurrent calls. For example, if you want to allow six calls at a time, enter 6.
	Overflow check	If selected, the phone calls exceeding the *Max channel* limit will be handled according to the call handling actions set in the dialplan applied to this trunk. If unselected, the phone calls exceeding the *Max channel* limit will be disconnected.
	Max outgoing channel	With known max channels, if you need to reserve incoming channels, you may enter the number of outgoing channels allowed and the remaining channels are for incoming calls. For example, the max channel number is 10 and you want to reserve 4 channels for incoming calls, you can enter 6 for *Max outgoing channel*.
	User=Phone in SIP URI	Select if your service provider requires this option to make the FortiVoice Gateway to be compatible with the VoIP service provider's configurations.
	Inband ringtone	Select to enable the FortiVoice Gateway to send a ring tone to the caller of an incoming call before establishing a call connection.
	Caller ID Option	Select if you want the trunk's main number to appear on the called phone. See Main number on page 43. Otherwise, the user name provided by the VoIP service provider for the FortiVoice Gateway to register with the SIP server will appear on the called phone. See User name on page 43.
	Registration	Enter the SIP registration information from the VoIP service provider by selecting a registration method. You can receive calls after registering with the SIP server of the VoIP service provider. • *Disable*: Select to deactivate the registration with the VoIP service provider.

GUI field	Description

	• *Standard*: Select to use the standard registration method which automatically registers with the SIP server of the VoIP service provider.
	• *Registrar*: Select to enter the registration information from the VoIP service provider:
	   • *Registrar host/IP*: Enter the VoIP service provider's SIP registration server domain name or IP address. For example, `172.20.120.11` or `voip.example.com.`
	   • *Registrar port:* Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number.
	   • *Transport protocol*: Select the transport protocol used for the registration.
	• *Registration URI*: Enter the registration string provided by the VoIP service provider in the *Registration URI* field.
	The string usually has the following formats:
	`register => user[:secret[:authuser]]@host [:port][/extension]`
	or
	`register => fromuser@fromdomain:secret@host`
	or
	`register => fromuser@fromdomain:secret: authuser@host:port/extension`
	For example, a string could be: `register => 2345:password@mysipprovider.com/1234`
	• *Registration interval*: Enter the time interval in minutes to register with the SIP server of the VoIP service provider.

Outbound Proxy	Some VoIP service providers use proxy servers to direct their traffic. If this is the case, your registration request will go to the proxy server first before reaching the registration server. Configure the following: • Select to activate the proxy server settings. • *Proxy (Host/IP)*: Enter the proxy server's domain name or IP address. For example, `172.20.120.11` or `voip.example.com.` • *Proxy port*: Enter the port number of the proxy server. • *Transport protocol*: Select the transport protocol used for the registration.
Phone Number	Click *New* to add the phone number provided by your VoIP service provider. The VoIP service provider SIP server will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Testing SIP trunks

After you create a SIP trunk, you can select the trunk and click *Test* to see if the trunk works.

To test a SIP trunk

1. Go to *Gateway > SIP > SIP.*
2. Select the trunk that you want to test and click *Test*.
3. Select *Test Call - Dry Run* or *Test Call*.
4. Configure the following fields, as applicable:

GUI field		Description
Test Call - Dry Run		Run a system SIP trunk test without making a real phone call.
	Destination number	Enter a destination number to call.
	From number	Enter the number from which you want to call the destination number. The FortiVoice Gateway will connect this number with the destination number for the test.
	Test	Click to start the dry run test and check the *Test result*.
	Reset	Click to remove the test result in order to start a new test.
Test Call		Test the SIP trunk by making a real phone call.
	Destination number	Enter a destination number to call.
	After call is established	Select the FortiVoice Gateway action once it calls the destination number: • *Play welcome message*: The FortiVoice Gateway will play a message to the destination number. • *Connect test call to number*: In the *Number* field, enter the number from which you want to call the destination number. The FortiVoice Gateway will connect this number with the destination number to test the trunk.
	Test	Click to start the test and check the *Test result*.
	Reset	Click to remove the test result in order to start a new test.

Creating a SIP trunk with FortiCall service

You can create one trunk with FortiCall and use it free for 30 days or 300 minutes, whichever comes first. Note that the trial account only allows outbound calling and no international calling is available.

If you sign up for the service during a trial use, the trial is closed and billing starts.

To create a SIP trunk with FortiCall service

1. Go to *Gateway > SIP > SIP.*
2. Click *FortiCall*.
   The *Create SIP Trunk* dialog box displays.
3. Take note of the *MAC Address* and *System ID* for use if you decide to sign up for the service later.

4. Keep *Create dialplans for this trunk* selected unless you want to create the dialplans by yourself.
The auto-generated dialplans will replace the default inbound, outbound, and emergency call dialplans. You can delete them if you do not choose to use the FortiCall service.
5. Click *OK*.
6. Enter your name, email address, and reseller or partner code.
7. Click *Create*.
8. Click *OK*.
The FortiCall trunk is created.

Configuring SIP profiles

Configure the SIP related settings and codecs and apply them to SIP trunks.

> Communicate with your VoIP service provider because the profile settings are subject to the capabilities of the VoIP service provider. For example, if some of your features and codecs are not supported by your VoIP service provider, they will not work even if they are enabled or selected in the SIP profile.

You can edit the default SIP profiles but you cannot delete them.

To configure a SIP profile

1. Go to *Gateway > SIP > Profile*.
2. Click *New*.
3. Select *Trunk*.

4. Configure the following fields:

GUI field	Description
Name	Enter a name for this profile.
DTMF	Select the dual-tone multi-frequency (DTMF) method used by the VoIP provider. Options are RFC2833, Inband, Info, Shortinfo, and Auto. Auto means the VoIP provider's server and the FortiVoice Gateway will negotiate to select a DTMF method. You could also select a specific DTMF method if required.
Keep alive	Enter the time interval in seconds for the FortiVoice Gateway to talk to the SIP server of your service provider to keep the connectivity and check its capability. A value of 0 (zero) means no checking by the FortiVoice Gateway.
NAT	Select if the VoIP service provider supports SIP NAT translation.
T.38	Select if the VoIP service provider supports fax over VoIP network.
Registration interval	To keep the extensions' registration status with the FortiVoice unit, keep the default value of extension registration time interval or enter the value in seconds as required by the FortiVoice unit. The default is 1800. The range is 10 - 28800.
Subscription interval	To keep the extensions' subscription status with the FortiVoice unit, keep the default value of extension subscription time interval or enter the value in minutes as required by the FortiVoice unit. . The default is 60. The range is 10 - 1440.
Transport	*Transport*: SIP commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for non-encrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS). Enable the protocols as required. *Secure RTP*: Select to provide encryption, message authentication and integrity, and replay protection to the FortiVoice Gateway Real-time Transport Protocol data.
Codec	Select the audio and video codecs supported by the VoIP service provider. Among the selected ones, choose the preferred one for the VoIP provider. The preferred codec is usually the most used one in your area and provides the best quality of communication. If your preferred codec is different from that of your VoIP service provider, the service provider's codec will be used as long as it is one of your supported codecs.

5. Click *Create*.

Adding analog trunks (GO04 and GO08 only)

The analog FXO (Foreign eXchange Office) ports connect your FortiVoice Gateway to your PSTN service providers and through them to the outside world.

To view the analog trunks, go to *Gateway > Analog*. The following table includes the GUI fields and descriptions.

GUI field	Description

Delete	Select to delete a trunk. To do so, you first need to remove the managed extensions using the following CLI commands on the FortiVoice console:
	`config extension user`
	      `delete the_mgd_ext`
	      (where `the_mgd_ext` is the managed extension ID to be removed. For example, ext1)
	Repeat this step to remove all the managed extensions.

Enabled	Select to activate the trunk.
Name	The name of the trunk.
Status	The trunk statuses, including: • *In service*: The trunk is currently in use. • *Not activated*: The trunk is not enabled. • *Idle*: The trunk is not in use. • *Unavailable*: The trunk is not reachable. • *Conflict*: The trunk conflicts with another one. • *Alarm detected*: There is a problem with the trunk. • *Admin down*: The trunk is disabled.
Type	The trunk type: analog.

To add an analog trunk

1. Go to *Gateway > Analog.*
2. Click *New*.
3. Configure the following:

GUI field		Description
Trunk Setting		
	Enabled	Select to activate the trunk.
	Name	Enter a name for the trunk.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Number	Enter the phone number that will appear on the called phone.
Hardware Property		
	Port	Select the FXO ports you want for this trunk and click -> to move them into the *Selected ports* field. Each FXO port selected provides a connection for this particular analog trunk profile. For example, if four FXO ports have been selected, this particular profile could allow up to four PSTN connections.
	Max channel	Displays the number of FXO ports that have been selected, and are available to receive incoming and outgoing calls.

GUI field	Description
Max outgoing channel	Defines how many of the FXO ports available can be used for outbound calls at one time.
Phone Number	Click *New* to add the phone number provided by your PSTN service provider. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

To edit PSTN settings for an analog trunk

Edit the PSTN settings to match the ones from your PSTN service provider.

1. Go to *Gateway > Analog.*
2. Select a trunk.
3. Click *PSTN Setting*.
4. Configure the following:

GUI field	Description
Name	The name of this configuration. This field is view-only.
Codec	Select the codec for the trunk.
Caller ID Signaling	Select the caller ID signaling standard per your phone company's request.

5. Click *OK*.

Editing analog extensions (GS04, GS16, and GS24 only)

The analog FXS (Foreign eXchange Subscriber) ports connect your FortiVoice Gateway to your PSTN service providers and through them to the outside world.

Depending on the model, the FortiVoice Gateway has 4,16, or 24 analog ports and 4, 16, or 24 default analog extensions. You can edit the extensions' default configuration.

Analog lines, also referred to as POTS (Plain Old Telephone Service), are used for standard phones, fax machines, and modems.

To edit a default analog extension

1. Go to *Gateway > Extension > Analog Extension.*
2. Select a default extension and click *Edit*.
3. Configure the following:

GUI field	Description
Enabled	Select to activate the extension.
Number	Enter the extension number following the extension number pattern.

GUI field	Description
User ID	This is the system-generated ID for the extension and is read-only.
Analog port	Select the analog port number. By default, it is *fxs1*.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.
Description	Add any notes for the extension.
User Setting	
Management	Configure the extension's role in other settings.
User privilege	Select the services for the extension. Click *Edit* to modify the current user privilege or click *New* to configure a new one.
Department	Select the department that the extension belongs to.
Voicemail	Configure the extension's voicemail. In some cases, you may want other users or groups to share this voicemail. For example, a supervisor wants his/her co-workers to access his/her voicemail while he/she is away. *Main voicemail:* Select the extension's own voicemail (*Default*) or that of another extension as the voicemail of this extension. Typically, you use the default voicemail. If you select the voicemail of another extension, you can click *Edit* to modify that extension. *Users/Groups*: The FortiVoice Gateway turns on the message waiting light on the phones of a user or user group to notify the user or group of a new voice message stored in the voicemail associated with this extension. To select users or user groups, under *User(s)* and *Group(s)*, click +, select the entries, and click Close. To listen to the message after being notified, the user can dial *97 or the code you set and enter the user's own user PIN.
Advanced	Click to configure desktop phone: • *Direct call*: Enable or disable direct calling on the phone. • *Number*: Enter a phone number. This is the phone number that FortiVoice automatically dials after the phone user lifts the phone handset (or presses the headset or speaker button) to place a call. • *DTMF passthrough*: Enable or diable DTMF (Dual Tone Multi-frequency).
Web Access	Configure the access to the user portal and softclient access from mobile or desktop devices.
Authentication type	Select the extension's authentication type: *Local* or *LDAP*.
User password	This option is only available when you select *Local* as the *Authentication Type*. Enter the password for user portal access which can be much longer and stronger to mitigate the risk of password guess attack and preserve the User PIN for phone access only.

GUI field	Description
	The control of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. You can check the password strength. To generate a strong password automatically, click *Generate.* To show the user password, click the eye icon.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP profile to apply to this extension.
Authentication ID	This option is only available if you select *LDAP* for *Authentication type*. If you select *Try common name with base DN as bind DN* as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects' common name attribute you entered in the *Common name ID* field of the profile, such as `jdoe`. If you select *Search user and try bind DN* as the user authentication option in the authentication profile you select, leave this field blank.
Phone Access	Configure voicemail access by phone or access to restricted phone calls.
Voicemail PIN	Enter the password for the extension user to access voicemail and the user web portal. Selection of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. To generate a strong password automatically, click *Generate*. To show the PIN, click the eye icon. If you have configured the default user PIN, the password appears here. However, you can change it.
Personal code	Enter the extension specific account code that can be used to restrict calls. This code is needed to make some restricted calls. To get a code, click *Generate*.

4. Click *OK*.

To edit PSTN settings for an analog extension

Edit the PSTN settings to match the ones from your PSTN service provider.

1. Go to *Gateway > Extension > Analog Extension.*
2. Select an extension.
3. Click *PSTN Setting*.

4. Configure the following:

GUI field	Description
Name	The name of this configuration. This field is view-only.
Codec	Select the codec for the extension.
Caller ID Signalling	Select the caller ID signalling standard per your phone company's request.
First digit Timeout Match digit Timeout	Enter the timeout in milliseconds. The following example explains both timeout settings using default values. The user picks up the phone handset and hears a dialtone. If the user does not enter a digit within the specified 16 seconds (first digit timeout), the dialtone restarts. After pressing the first digit, the user has 3 seconds (match digit timeout) to enter the next digit. After the user's finger is off the button, the timer resets and the user has another 3 seconds to enter the next digit and so on. When the 3-second timer expires, the phone number is identified as complete, and the call is attempted. The default *First digit Timeout* is 16000. The default *Match digit Timeout* is 3000.

5. Click *OK*.

Adding PRI trunks (GT01 & GT02 only)

FortiVoice Gateway Primary Rate Interface (PRI) carries multiple DS0 voice and data transmissions to your PRI service providers and through them to the outside world.

To view the PRI trunks, go to *Gateway > PRI*. The following table includes the GUI fields and descriptions.

GUI field	Description
Enabled	Select to activate the trunk.
Name	The name of the trunk.
Status	The trunk statuses, including: • *In service*: The trunk is currently in use. • *Not activated*: The trunk is not enabled. • *Idle*: The trunk is not in use. • *Unavailable*: The trunk is not reachable. • *Conflict*: The trunk conflicts with another one. • *Alarm detected*: There is a problem with the trunk. • *Admin down*: The trunk is disabled.
Type	The trunk type: analog.

To add a PRI trunk

1. Go to *Gateway > PRI.*
2. Click *New*.

3. Configure the following:

GUI field		Description
Trunk Setting		
	Enabled	Select to activate the trunk.
	Name	The name of this trunk. This is view only.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Number	Enter the phone number that will appear on the called phone.
Hardware Property		Use this option to configure the T1/E1 span. Spans represent trunks (spans) of T1/E1 PSTN lines. FortiVoice supports T1/E1 lines according to the installed voice card. You can add a span name using the CLI.
	Edit span	Select the span you want to modify and click the *Edit* icon. For more information, see Configuring the T1/E1 span on page 54.
	Span	Use this option to configure the PRI trunk. Select a span in the *Available* field and click -> to move it into the *Selected* field.
	Max channel	Indicates the total number of B channels of the spans.
	Max outgoing channel	Enter the number of outgoing channels out of the maximum number of B channels.
Phone Number		Click *New* to add the phone number provided by your PSTN service provider. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *OK*.

Configuring the T1/E1 span

You can configure the settings of the T1/E1 span, including full or fractional PRI (T1/E1), to match the same settings of your PSTN service provider.

> For GT02, if a PRI trunk includes two spans, the configuration of the second span is much simpler as the spans share many configurations.

For more information, see Hardware Property on page 54.

To configure the T1/E1 span

1. Go to *Gateway > PRI*.
2. Select a span name and click *Edit*.

3. For *Edit span* under *Hardware Property*, select a span and click the *Edit* icon.
4. Configure the following:

GUI field		Description
Standard Options		
	Name	The name of this span. This is view-only.
	Type	Select the span type: *PRI T1* or *PRI E1*. A T1 span usually supports 23+1 channels, while an E1 span supports 30 channels in CAS (Channel Associate Signaling) mode and 30 B channels and one D channel in ISDN mode.
	Signalling	Select the signaling type of the ISDN PRI: • *PRI signalling, CPE* (Customer Premises Equipment) *side* • *PRI signalling, Network Side* • *PRI R2 signalling*
Advanced Options		
	Framing and coding options	Specify the type of framing and coding to provision the PRI with your PSTN service provider.
	Clocking options	Select the FortiVoice unit's clock synchronization: • Clock sourcing from PSTN network • Internal clocking source This option does not need to match that of your PSTN service provider.
	Receive sensitivity	Select the level of receiver sensitivity. The receiver sensitivity is the ability of the phone receiver to pick up the required level of phone signals to make it operate more effectively within its application. This option does not need to match that of your PSTN service provider.
	D-channel signalling format	Select a signalling method for the D channel which is a signalling channel and carries the information needed to connect or disconnect calls and to negotiate special calling parameters (for example, automatic number ID, call waiting, data protocol). The D channel can also carry packet-switched data using the X.25 protocol.
	Line build out	Select the line build out (LBO). LBO settings are an inherent part of T1 and T3 network element transmission circuitry. Since cable lengths between network elements and digital signal cross-connect (DSX) vary in the central office, LBO settings are used to adjust the output power of the transmission signal to achieve equal level point (ELP) at the DSX.
	D-channel	By default, depending on your selection of , the typical channel numbers are: • Full T1: 24 • Full E1: 16

GUI field	Description
	You can also set the channel numbers to others such as 1. The settings you configure must match the same settings of your PSTN service provider.
B-channel	By default, depending on your selection of Type on page 55, the typical channel settings are: • Full T1: 1-23 • Full E1: 1-15, 17-31 You can also configure the fractional channel numbers. For example, for T1/E1, the channels can be: • 1-12 • 2, 3, 4, 9-15 • 2-4, 9-15 The settings you configure must match the same settings of your PSTN service provider.
Dialplan type (TON)	Select a number format for placing a call from FortiVoice to the service provider. The values for this option are provided by the service provider. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Signalling on page 55.
Local dialplan type (TON)	Select a number format for placing a call from the service provider to FortiVoice. The values for this option are provided by the service provider. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Signalling on page 55.
Connected party notification dialplan Type (TON)	Select a number format used in caller-ID and remote party ID (if supported by the service provider). The values for this option are provided by the service provider. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Signalling on page 55.
PRI indication	Select a value that is typically provided by the service provider. However, some providers allow this value to be set on the PBX. • In Band: Call failure tones, for example, busy signal and out of service messages, are played back as audio from the service provider. • Out of Band: Call failure tones are generated by FortiVoice with the service provider sending a code instead of a tone. This is required for some automated dialing scenarios, but you will often lose extra information that may be included in the recorded message. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Signalling on page 55.
PRI R2 Setting	Since there is no single signaling standard for R2, the FortiVoice Gateway addresses this challenge by supporting many localized implementations of R2 signaling.

GUI field	Description
	This option is active only if you select PRI R2 signalling for Signalling on page 55.
Country	Select the country for PRI R2 settings.
Max ANI digits	Automatic Number Identification (ANI) is a system used by telephone companies to identify the Directory Number (DN) of a calling subscriber. It allows subscribers to capture or display a caller's telephone number. Enter the number of digits of a caller's phone number to capture.
Max DNIS digits	Dialed Number Identification Service (DNIS) is a service provided by telephone companies that lets the subscribers determine which telephone number was dialed by a caller. Enter the number of digits of a dialed call to be sent by the telephone company.
Caller category	Select the caller type.
Incoming digits mode	Select the incoming digits mode by consulting your telephone company.
DMTF option DTMF dialing	Select to enable dual-tone multi-frequency signaling (DTMF) dialing.
DTMF answering	Select to enable dual-tone multi-frequency signaling (DTMF) answering.
Allow collect calls	Select to allow collect calls.
MF timeout	To enable the multi-frequency (MF) timeout, enter a value in milliseconds. The default is -1, which disables the setting.
Metering pulse timeout	To enable the metering pulse timeout, enter a value in milliseconds. The default is -1, which disables the setting.

5. Click *OK*.

Mapping a SIP peer with the FortiVoice Gateway

Mapping Rule allows for calls to be made from a SIP peer to the FortiVoice Gateway and then out on an analog trunk. Likewise, calls can come in on an analog trunk and be answered through the SIP peer. When creating a mapping rule, you are linking the analog trunks to the SIP peer or link analog extensions to SIP peers, depending on the platform.

To add a mapping rule

1. Go to *Gateway > Mapping Rule.*
2. Click *New*.
3. Configure the following fields:

GUI field	Description
Enabled	Select to activate the rule.
PSTN trunk (GO08 only)	Select the analog trunk profile that you want to map to the SIP peer.
SIP peer	Select the SIP trunk profile that you want to map to the PSTN trunk.
PRI trunk (GT01 & GT02 only)	Select the PRI trunk profile that you want to map to the SIP peer.
Extension (GS16 only)	Select the analog extension that you want to map to the SIP peer.
Comments	Enter any comments you have for this mapping rule.

4. Click *Create*.

Configuring logs

The *Log & Report* menu lets you configure FortiVoice Gateway logging.

FortiVoice Gateway provides extensive logging capabilities for voice incidents and system events. Detailed log information provides analysis of network activity to help you identify network issues and reduce network misuse and abuse.

Logs are useful when diagnosing problems or when you want to track actions the FortiVoice Gateway performs as it receives and processes phone calls.

This section includes the following topics:

About FortiVoice Gateway logging

FortiVoice Gateway can log multiple events. See FortiVoice Gateway log types on page 59.

You can select which severity level an activity or event must meet in order to be recorded in the logs. For more information, see Log message severity levels on page 60.

A FortiVoice Gateway can save log messages to its hard disk.

This topic includes:

FortiVoice Gateway log types

FortiVoice Gateway can record system, voice, and fax log messages. You can view these logs from the *Monitor > Log*.

System logs include the following types:

- Administration
- Configuration
- DHCP
- DNS
- HA
- Monitor
- System
- Web Mail

Avoid recording highly frequent log types such as voice logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as `warning`.

Log severity levels

Level	Description
0 - Emergency	Indicates the system has become unusable.
1 - Alert	Indicates immediate action is required.
2 - Critical	Indicates functionality is affected.
3 - Error	Indicates an error condition exists and functionality could be affected.
4 - Warning	Indicates functionality could be affected.
5 - Notification	Provides information about normal events.
6 - Information	Provides general information about system operations.

For each location where the FortiVoice Gateway can store log files, you can define the severity threshold of the log messages to be stored there.

Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is a possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

The FortiVoice Gateway stores all log messages equal to or exceeding the severity level you select. For example, if you select *Error*, the FortiVoice Gateway stores log messages whose severity level is *Error*, *Critical*, *Alert*, or *Emergency*.

Configuring logging

The *Log & Report > Log Setting* submenu includes two tabs, *Local and Remote*, that let you:

- set the severity level
- configure which types of log messages to record
- specify where to store the logs

You can configure the FortiVoice Gateway to store log messages locally (that is, in RAM or to the hard disk), remotely (that is, on a Syslog server or FortiAnalyzer unit), or at both locations.

Your choice of storage location may be affected by several factors, including the following:

- Local logging by itself may not satisfy your requirements for off-site log storage.
- Very frequent logging may cause undue wear when stored on the local hard drive. A low severity threshold is one possible cause of frequent logging. For more information on severity levels, see Log message severity levels on page 60.

For information on viewing locally stored log messages, see Viewing log messages on page 14.

This section includes the following topics:

- Configuring logging to the hard disk on page 61
- Configuring logging to a Syslog server or FortiAnalyzer unit on page 62

Configuring logging to the hard disk

You can store log messages locally on the hard disk of the FortiVoice Gateway.

To ensure that the local hard disk has sufficient disk space to store new log messages and that it does not overwrite existing logs, you should regularly download backup copies of the oldest log files to your management computer or other storage, and then delete them from the FortiVoice Gateway.

You can view and download these logs from the *Log* submenu of the *Monitor* tab. For more information, see Viewing log messages on page 14.

For logging accuracy, you should also verify that the FortiVoice Gateway's system time is accurate. For details, see Configuring the time and date on page 26.

To configure logging to the local hard disk

1. Go to *Log & Report > Log Setting > Local*.
2. Select *Enabled* to allow logging to the local hard disk.
3. In *Log file size*, enter the file size limit of the current log file in megabytes (MB). The log file size limit must be between 10 MB and 1000 MB.
4. In *Log time*, enter the time (in days) of file age limit.
5. In *At hour*, enter the hour of the day (24-hour format) when the file rotation should start.
   When a log file reaches either the age or size limit, the FortiVoice Gateway rotates the current log file: that is, it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, and so on), then creates a new current log file. For example, if you set the log time to 10 days at hour 23, the log file will be rotated at 23 o'clock of the 10th day.

   > Large log files may decrease the display and search performance.

6. In *Log level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.
7. In *Log options when disk is full*, select what the FortiVoice Gateway will do when the local disk is full and a new log message is caused, either:
   - *Overwrite*: Delete the oldest log file in order to free disk space, and store the new log message.
   - *Do Not Log*: Discard all new log messages.

8. In *Logging Policy Configuration*, enable the types of logs that you want to record to this storage location.

Log type	Description
System	Includes system and administration events, such as downloading a backup copy of the configuration.
Generic	Includes the following events: • SMTP relay or proxy events • Voice user login and logout events
Voice	Includes phone calls events.
DTMF (Enhanced CDR)	Includes DTMF (Dual Tone Multi-Frequency) events.

9. Click *Apply*.

Configuring logging to a Syslog server or FortiAnalyzer unit

Instead of or in addition to logging locally, you can store log messages remotely on a Syslog server or a FortiAnalyzer unit.

You can add a maximum of three remote Syslog servers.

> Logs stored remotely cannot be viewed from the GUI of the FortiVoice Gateway. If you require the ability to view logs from the GUI, also enable local storage. For details, see Configuring logging to the hard disk on page 61.

Before you can log to a remote location, you must first enable logging and choose which events to log. For details, see Configuring logging to the hard disk on page 61. For logging accuracy, you should also verify that the FortiVoice unit's system time is accurate. For details, see Configuring the time and date on page 26.

To configure logging to a Syslog server or FortiAnalyzer unit

1. Go to *Log & Report > Log Setting > Remote*.
2. Click *New* to create a new entry or double-click an existing entry to modify it.

GUI field	Description
Enabled	Select to allow logging to a remote host.
Name	Enter a name for the remote host.
IP	Enter the IP address of the Syslog server or FortiAnalyzer unit where the FortiVoice Gateway will store the logs.
Port	If the remote host is a FortiAnalyzer unit, enter 514; if the remote host is a Syslog server, enter the UDP port number on which the Syslog server listens for connections (by default, UDP 514).
Level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location.

GUI field	Description
	For information about severity levels, see Log message severity levels on page 60.
Facility	Select the facility identifier that the FortiVoice Gateway will use to identify itself when sending log messages. To easily identify log messages from the FortiVoice Gateway when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.
CVS format	Enable this option if you want to send log messages in comma-separated value (CSV) format. Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages.
Logging Policy Configuration	Click the arrow to review the options and enable the types of logs you want to record to this storage location. For details, see step 8 of Configuring logging to the hard disk on page 61.

3. Click *Create*.
4. If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiVoice Gateway was added to the FortiAnalyzer unit's device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer unit. For details, see the FortiAnalyzer Administration Guide.
5. To verify logging connectivity, from the FortiVoice Gateway, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

    For example, if you have chosen to record event log messages to the remote host and if they are more severe than Information, you could log in to the GUI or download a backup copy of the FortiVoice Gateway's configuration file in order to trigger an event log message.

    If the remote host does not receive the log messages, verify the FortiVoice Gateway's network interfaces (see Configuring the network interfaces on page 18) and static routes (see Configuring static routes on page 21), and the policies on any intermediary firewalls or routers. If ICMP ECHO (ping) is enabled on the remote host, you can use the `execute traceroute` command to determine the point where connectivity fails.

Configuring alert email messages

The *Alert* submenu lets you configure the FortiVoice Gateway to notify selected users (including administrators) by email when specific types of events occur and are logged. For example, if you require notification about system activity event detections, you can have the FortiVoice Gateway send an alert email message whenever the FortiVoice Gateway detects a system activity event.

To set up alerts, you must configure both the alert email recipients (see Configuring alert recipients on page 64) and which event categories will trigger an alert email message (see Configuring alert categories on page 64).

Alert email messages also require that you supply the FortiVoice Gateway with the IP address of at least one DNS server. The FortiVoice Gateway uses the domain name of the SMTP server to send alert email messages. To resolve

this domain name into an IP address, the FortiVoice Gateway must be able to query a DNS server. For information on DNS, see Configuring DNS on page 22.

This topic includes:

- Configuring alert recipients on page 64
- Configuring alert categories on page 64

Configuring alert recipients

Before the FortiVoice Gateway can send alert email messages, you must create a recipient list.

To configure recipients of alert email messages

1. Go to *Log & Report > Alert > Configuration*.
2. Click *New* to add the email address of a recipient.
3. In *Email to*, enter a recipient email address.
4. Click *Create*.
5. To add more users, repeat steps 2 to 4.

To test the alert email

1. Make sure that the list of Alert Email Account shows the configured recipients.
2. Click **Test**.
3. Contact the recipients to confirm that they have received the alert email.

Configuring alert categories

Before the FortiVoice Gateway can send alert email messages, you must specify which events cause the FortiVoice Gateway to send an alert email message to your list of alert email recipients (see Configuring alert recipients on page 64).

To select events that will trigger an alert email message

1. Go to *Log & Report > Alert > Category*.
2. Select one or more of the following event categories check boxes:

GUI field	Description
Alert Email Setting	
Critical events	Send an alert email message when the FortiVoice Gateway unit detects a system error that may affect its operation.
Disk is full	Send an alert email message when the hard disk of the FortiVoice Gateway unit is full.
FXO alarm (for GO08 only)	Send an alert email when the PSTN analog line has a problem.
PRI alarm (for GT01 and GT02 only)	Send an alert email when the PRI line has a problem.
Trunk lines are saturated	Send an alert email when the SIP/PSTN/PRI trunk lines are fully occupied.

GUI field	Description
	SIP trunk alert only works if you select *Overflow check* when configuring SIP trunk.
Trunk	
SIP trunk/office peer connectivity alert	Select the trunks of which an alert email is sent when a trunk has an issue.
Alert interval	If you enable *SIP trunk/office peer connectivity alert*, then you can set the time interval (in seconds) for sending alert emails.

3. Click *Apply*.

Installing the firmware

Fortinet periodically releases FortiVoice Gateway firmware updates to include enhancements and address issues.

For information specific to the firmware release, see the Release Notes.

In addition to FortiVoice major releases that contain new features, FortiVoice patch releases focuses on resolving specific issues and may include new features and/or changes to existing features. Fortinet recommends that you download and install patch releases as soon as they are available.

Before you can download firmware updates for your FortiVoice Gateway unit, you must first register your FortiVoice Gateway with Fortinet Support. For details, see Registering your Fortinet product on page 6.

This section includes the following topics:

Downloading the firmware image file

Access the Fortinet Support website and download the firmware image file for the version that you want to upgrade to.

1. Go to the Fortinet Support website.
2. Log in to your existing account or register for an account.
3. Select *Support > Firmware Download*.
4. In *Select Product*, select *FortiVoice*.
5. Select the *Download* tab and navigate to the folder for the firmware version that you are upgrading to.
6. To download the firmware image file to your management computer, go to the end of the row and click HTTPS.
7. Save the file on your management computer.
8. Take note of the location where you save the file.

Testing a new firmware image

You can test a new firmware image before installing it by temporarily running that firmware image from memory, without saving it to disk. By keeping your existing firmware on disk, if the evaluation fails, you do not have to re-install your previous firmware. Instead, you can quickly revert to your existing firmware by simply rebooting the FortiVoice Gateway.

To test a new firmware image

1. Connect your management computer to the FortiVoice Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate a connection from your management computer to the CLI of the FortiVoice Gateway.
3. Connect port1 of the FortiVoice Gateway directly or to the same subnet as a TFTP server.
4. Copy the new firmware image file to the root directory of the TFTP server.
5. Verify that the TFTP server is currently running, and that the FortiVoice Gateway can reach the TFTP server.
   To use the FortiVoice Gateway CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
6. Enter the following command to restart the FortiVoice Gateway:
   ```
   execute reboot
   ```
7. As the FortiVoice Gateway starts, a series of system startup messages are displayed.
   ```
   Press any key to display configuration menu........
   ```
8. Immediately press a key to interrupt the system startup.

> ⚠️ You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiVoice Gateway reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.

[F]: Format boot device.

[B]: Boot with backup firmware and set as default.

[I]: Configuration and information.

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.


Enter G,F,B,I,Q,or H:
```

9. Type `G` to get the firmware image from the TFTP server.
   The following message appears:
   ```
   Enter TFTP server address [192.168.2.99]:
   ```
10. Type the IP address of the TFTP server and press Enter.
    The following message appears:
    ```
    Enter Local Address [192.168.2.99]:
    ```
11. Type a temporary IP address that can be used by the FortiVoice Gateway to connect to the TFTP server.
    The following message appears:
    ```
    Enter File Name [image.out]:
    ```
12. Type the firmware image file name and press Enter.
    The FortiVoice Gateway downloads the firmware image file from the TFTP server and displays a message similar to the following:
    ```
    Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
    ```

13. Type `R`.
    The FortiVoice Gateway image is loaded into memory and uses the current configuration, **without** saving the new firmware image to disk.
14. To verify that the new firmware image has been loaded, log in to the CLI and type:
    `get system status`
15. Test the new firmware image.
    - If the new firmware image operates successfully, you can install it to disk, overwriting the existing firmware, using the procedure Installing the firmware on page 68.
    - If the new firmware image does **not** operate successfully, reboot the FortiVoice Gateway to discard the temporary firmware and resume operation using the existing firmware.

Installing the firmware

If you are upgrading, the upgrade process may require a specific path. Very old versions of the firmware may not be supported by the configuration upgrade scripts that are used by the newest firmware. As a result, you may need to upgrade to an intermediate version of the firmware first, **before** upgrading to your intended version.

Before upgrading the firmware of the FortiVoice Gateway, review the Release Notes for the new firmware version. The Release Notes document includes the most current upgrade information such as the supported upgrade path and may contain details that were unavailable at the time this guide was created.

You can use either the GUI or the CLI to upgrade or downgrade the firmware of the FortiVoice Gateway.

Administrators whose access profile contains *Read-Write* access in the *Others* category, such as the `admin` administrator, can change the FortiVoice Gateway firmware.

Firmware changes are either:

- An upgrade to a newer version.
- A reversion to an earlier version.

To determine if you are upgrading or reverting your firmware image, examine the firmware version number. To access the firmware version in the FortiVoice Gateway GUI, go to *Dashboard > Status* and the *System Information* widget. You can find the firmware version details in the *Firmware version* row. For example, if your current firmware version is `v6.4.5,build446` and you are changing to `v6.4.7,build477`, a later build number, indicates that you are upgrading.

To install the firmware using the GUI

Before upgrading or downgrading, make sure to back up the configuration and call data. For details, see Backing up the configuration on page 39.

Reverting to an earlier firmware version may cause the FortiVoice Gateway to remove parts of the configuration that are not valid for that earlier version. In some cases, you may lose all call data and configurations.

1. Log in to the Fortinet Support website.
2. Download the firmware image file to your management computer.
3. Log in to the GUI as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Go to *Dashboard > Status*.
5. In the *System Information* widget, go to the *Firmware version* row, and click *Update*.
6. Click *Browse* to locate the firmware and then click *Upload*.
   Your web browser uploads the firmware file to the FortiVoice Gateway. The FortiVoice Gateway installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.
   If you are downgrading the firmware to a previous version, the FortiVoice Gateway reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVoice Gateway or restore the configuration file.
7. Clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all changes.
8. To verify that the firmware was successfully installed, log in to the web UI and go to *Dashboard > Status*. Text appearing in the *Firmware version* row indicates the currently installed firmware version.

To install the firmware using the CLI

1. Log in to the Fortinet Support website.
2. Download the firmware image file to your management computer.
3. Connect your management computer to the FortiVoice Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
4. Initiate a connection from your management computer to the CLI of the FortiVoice Gateway, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
5. Connect port1 of the FortiVoice Gateway directly or to the same subnet as a TFTP server.
6. Copy the new firmware image file to the root directory of the TFTP server.
7. Verify that the TFTP server is currently running, and that the FortiVoice Gateway can reach the TFTP server.
   To use the FortiVoice Gateway CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
8. Enter the following command to download the firmware image from the TFTP server to the FortiVoice Gateway:
   ```
   execute restore image tftp <name_string> <tftp_ipv4>
   ```
   where `<name_string>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.2.99, enter:
   ```
   execute restore image tftp image.out 192.168.2.99
   ```
   One of the following messages appears:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
   or:
   ```
   Get image from tftp server OK.
   Check image OK.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```
9. Type `y`.
   The FortiVoice Gateway downloads the firmware image file from the TFTP server. The FortiVoice Gateway installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

If you are downgrading the firmware to a previous version, the FortiVoice Gateway reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVoice Gateway or restore the configuration file.

10. If you also use the GUI, clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all tab, button, and other changes.

11. To verify that the firmware was successfully installed, log in to the CLI and type:

    ```
    get system status
    ```

12. If you have downgraded the firmware version, reconnect to the FortiVoice Gateway using its default IP address for port1, 192.168.1.99, and restore the configuration file. For details, see Reconnecting to the FortiVoice Gateway on page 70 and Restoring the configuration on page 71.

    If you have upgraded the firmware version, to verify the conversion of the configuration file, see Verifying the configuration on page 72. If the upgrade is unsuccessful, you can downgrade the firmware to a previous version.

Reconnecting to the FortiVoice Gateway

After downgrading to a previous firmware version, the FortiVoice Gateway reverts to default settings for the installed firmware version, including the IP addresses of network interfaces through which you connect to the FortiVoice Gateway GUI, CLI, or both.

To reconnect using the CLI

1. Connect your management computer to the FortiVoice Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.

2. Start a terminal emulation software (such as PuTTY).

3. Enter a name for the connection and click *OK*.

4. Configure the terminal emulation software to connect directly to the communications (COM) port on your computer and click *OK*.

5. Select the following port settings and click *OK*:

Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press Enter to connect to the FortiVoice Gateway CLI.
   The login prompt appears.

7. Type `admin` and press Enter twice.
   The following prompt appears:

    ```
    Welcome!
    ```

8. Enter the following command:

    ```
    set system interface <interface_string> mode static ip <address_ipv4> <mask_ipv4>
    ```
   where:

   - `<interface_string>` is the name of the network interface, such as `port1`
   - `<address_ipv4>` is the IP address of the network interface, such as 192.168.1.10
   - `<mask_ipv4>` is the netmask of the network interface, such as 255.255.255.0

   Enter the following command:

```
set system interface <interface_string> config allowaccess <accessmethods_string>
```
where:

- `<interface_string>` is the name of the network interface configured in the previous step, such as `port1`
- `<accessmethods_string>` is a space-delimited list of the administrative access protocols that you want to allow on that network interface, such as `ping ssh https`

The IP address and netmask of the network interface are saved. You can now reconnect to either the web UI or CLI using that network interface. For information about restoring the configuration, see Restoring the configuration on page 71.

Restoring the configuration

You can restore a backup copy of the configuration file from your local PC using either the GUI or CLI. For information about configuration backup, see Backing up the configuration on page 39.

If you have just downgraded or restored the firmware of the FortiVoice Gateway, restoring the configuration file can be used to reconfigure the FortiVoice Gateway from its default settings.

To restore the configuration file using the web UI

1. Clear your browser's cache. If your browser is currently displaying the GUI, also refresh the page.
2. Log in to the GUI.
3. Go to *System > Maintenance > Configuration*.
4. Under *Restore Configuration*, click *Browse* to locate and select the configuration file that you want to restore, then click *Restore*.
   The FortiVoice Gateway restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
5. After restoring the configuration file, verify that the settings have been successfully loaded. For details on verifying the configuration restoration, see Verifying the configuration on page 72.

To restore the configuration file using the CLI

1. Initiate a connection from your management computer to the CLI of the FortiVoice Gateway, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
2. Connect a network interface of the FortiVoice Gateway directly or to the same subnet as a TFTP server.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Verify that the TFTP server is currently running, and that the FortiVoice Gateway can reach the TFTP server.
   To use the FortiVoice Gateway CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
5. Enter the following command:
   ```
   execute restore config tftp <file_name> <tftp_ipv4>
   ```
   The following message appears:
   ```
   This operation will overwrite the current settings!
   (The current admin password will be preserved.)
   Do you want to continue? (y/n)
   ```
6. Enter `y`.
   The FortiVoice Gateway restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.

7. After restoring the configuration file, verify that the settings have been successfully loaded. For details on verifying the configuration restoration, see Verifying the configuration on page 72.

Verifying the configuration

After installing a new firmware file, you should verify that the configuration has been successfully converted to the format required by the new firmware and that no configuration data has been lost.

In addition to verifying successful conversion, verifying the configuration also provides familiarity with new and changed features.

To verify the configuration upgrade

1. Clear your browser's cache and refresh the login page of the GUI.
2. Log in to the GUI using the `admin` administrator account.
   Other administrator accounts may not have sufficient privileges to completely review the configuration.
3. Review the configuration and compare it with your configuration backup to verify that the configuration has been correctly converted.

Performing a clean firmware installation

Performing a clean firmware installation can be useful if:

- You are unable to connect to the FortiVoice Gateway using the web-based manager or the CLI.
- You want to install firmware **without** preserving any existing configuration.
- A firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware).

Unlike upgrading or downgrading firmware, performing a clean firmware installation re-images the boot device. Also, a clean installation can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. **A clean installation cannot be done through a network connection.**

	A clean installation resets the configuration, including the IP addresses of network interfaces. Before beginning this procedure, back up your configuration, if possible. For information about backups, see Backing up the configuration on page 39. For information about reconnecting to a FortiVoice Gateway whose network interface configuration has been reset, see Reconnecting to the FortiVoice Gateway on page 70.

	If you are reverting to a previous FortiVoice Gateway version, you may not be able to restore your previous configuration from the backup configuration file.

To perform a clean firmware installation

1. Download the firmware file from the Fortinet Support website.
2. Connect your management computer to the FortiVoice Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
3. Initiate a **local console connection** from your management computer to the CLI of the FortiVoice Gateway, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Connect port1 of the FortiVoice Gateway directly to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. Verify that the TFTP server is currently running, and that the FortiVoice Gateway can reach the TFTP server.
   To use the FortiVoice Gateway CLI to verify connectivity, if it is responsive, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
7. Enter the following command to restart the FortiVoice Gateway:
   ```
   execute reboot
   ```
   or power off and then power on the FortiVoice Gateway.
8. As the FortiVoice Gateway starts, a series of system startup messages are displayed.
   ```
   Press any key to display configuration menu........
   ```
9. Immediately press a key to interrupt the system startup.

> ⚠️ You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiVoice Gateway reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appear:
```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.


Enter G,F,B,I,Q,or H:
```
10. If the firmware version requires that you first format the boot device before installing firmware, type `F`. (Format boot device) before continuing.
11. Type `G` to get the firmware image from the TFTP server.
    The following message appears:
    ```
    Enter TFTP server address [192.168.2.99]:
    ```
12. Type the IP address of the TFTP server and press Enter.
    The following message appears:
    ```
    Enter Local Address [192.168.1.188]:
    ```
13. Type a temporary IP address that can be used by the FortiVoice Gateway to connect to the TFTP server.
    The following message appears:
    ```
    Enter File Name [image.out]:
    ```
14. Type the firmware image file name and press Enter.
    The FortiVoice Gateway downloads the firmware image file from the TFTP server and displays a message similar to the following:
    ```
    Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
    ```

15. Type `D`.

    The FortiVoice Gateway downloads the firmware image file from the TFTP server. The FortiVoice Gateway installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

    The FortiVoice Gateway reverts the configuration to default values for that version of the firmware.

16. Clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all tab, button, and other changes.

17. To verify that the firmware was successfully installed, log in to the CLI and type:

    ```
    get system status
    ```

    The firmware version number appears.

18. Either reconfigure the FortiVoice Gateway or restore the configuration file from a backup. For details, see Restoring the configuration on page 71.

www.fortinet.com